UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/763,079	01/22/2004	Daniel Brokenshire	AUS920030972US1	6481

50170 7590 07/31/2007

IBM CORP. (WIP)
c/o WALDER INTELLECTUAL PROPERTY LAW, P.C.
P.O. BOX 832745
RICHARDSON, TX 75083

EXAMINER	
ANWARI, MACEEH	

ART UNIT	PAPER NUMBER
2144	

MAIL DATE	DELIVERY MODE
07/31/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/763,079	BROKENSHIRE ET AL.	
	Examiner	Art Unit	
	Maceeh Anwari	~~2109~~ 2144	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 January 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15 and 18-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15 and 18-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: 0.

DETAILED ACTION

1. This action is responsive to the amendments filed 5/2/07. Claims 1, 6-7, 14, 18, 21-23 were amended. Claims 16 and 17 were canceled. No other claims have been amended, canceled, or newly presented. Accordingly, claims 1-15 and 18-23 are pending.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 22 and 23 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. More specifically, the applicant fails to sufficiently point out or describe computer readable media.

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 22-23 each fall under a judicial exception, an abstract idea, and are not directed to a practical application of such a judicial exception because they fail to produce a tangible result.

Furthermore, claims 22 and 23 disclose a computer program product, sharing the same above mentioned components, and failing to fall under one of the statutory categories. It is software per se and fails to provide a tangible result. As the applicant is attempting to claim a manufacture, the examiner notes that the claim is lacking a proper computer readable medium.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-15 and 18-23 are rejected under 35 U.S.C. 102(e) as being anticipated by Shrader, U.S. Patent No. 6,914,985.

Shrader teaches:

Claim 1:

A system for secure communication, comprising: a random value generator configured to generate a random value (Shrader Col. 11, lines 47-48; teaches this because the enveloped data is constructed and generated at random); a message validation code generator (Shrader Col. 2, lines 19-29 & Col. 13, line 57-67; states that the enveloped data have validation checks) coupled to the random value generator and configured to generate a message

validation code based on a predetermined key (Shrader Figure 3 & 4C & 7 & Col. 1, line 27-43; states how the Public-key cryptography standard is applied within his and other inventions), a message (Shrader Col. 2, lines19-40; teaches here that using the PKCS #7 one would be able to include encrypted messages), and the random value; a one-time pad generator coupled to the random number generator and configured to generate a one-time pad based on the random value and the predetermined key; and a masked message generator coupled to the one-time pad generator and configured to generate a masked message based on the one-time pad and the message (Shrader Col. 11, lines 65-67; meets the limitation of generating a masked message based on the one-time pad by stating that the encrypted content/data be padded to a multiple of some block size); and a transmitter configured to transmit a secure message that comprises the random value, the masked message, and the message validation code to a message target, wherein the message target is configured to unmask the masked message to form the message and validate the message using the message validation code (Col. 13 lines 57-67).

Claims 2- 4:

Wherein the message validation code generator (MVC), and the one-time pad generator (OTP), employs a first one-way hash function and wherein the MVC employs a first one-way hash function and the OTP employs a second one-way hash function (Shrader Col. 8, lines 31-35 & lines 62-67 & Col. 9, lines1-2 &

Col. 11, lines 47-48; teaches on the use of a single or multiple hash functions and or algorithms.)

Claim 5:

The system as recited in claim 1, further comprising a protected message envelope (PME) generator coupled to the random value generator (Col. 11, lines 46-47; meets the limitations of a PME and a random generator), the message validation code generator (Col. 2, lines 19-29 & Col. 13, lines 57-67; meets the limitations of a message validation process), and the masked message generator (Col. 13, lines 34-44; reads on an encryption messaging process), and configured to generate a protected message envelope based on the random value, the message validation code, and the masked message (the combination of the above sections and Figure 3 anticipate all the features within this claim).

Claim 6:

The system as recited in claim 5, wherein the transmitter is coupled to the protected message envelope generator and configured to transmit the protected message envelope to the message target (Col. 13, lines 57-67 & Col. 14, lines 1-7; reads on the limitations of the transmitter and transmission).

Claim 7:

A system in a message target for secure communication, comprising:

a receiver configured to receive a secure message transmitted from a message source, wherein the secure message comprises a protected message envelope;

a protected message envelope reader configured to receive the protected message envelope (Col. 12, lines 4-7 & Col. 15, lines 38-63; meets the limitations of protected message enveloped reader) and extract a random value, a masked message (Col. 11, lines 47-48 & 62-67 & Col. 12, lines 1-3; reads on the random value and the masked message components), and a first message validation code from the received protected message envelope, wherein the random value, the masked message, and the first message validation code are generated at the message source (Col. 2, lines 19-29 & Col. 13, lines 57-67; meets the limitation of the validation); a one-time pad generator coupled to the protected message envelope reader and configured to generate a one-time pad based on the random value and a predetermined key (Col. 11, lines 46-67; reads on the limitation of the pad and the key); and a message unmasker coupled to the one-time pad generator and protected message envelope reader, and configured to generate an unmasked message based on the one-time pad and the masked message (Col. 12, lines 4-7& 34-46 & Col. 15, lines 38-63; reads on the unmasking of the masked message)

Claim 8:

The system as recited in claim 7, wherein the one-time pad generator employs a first one-way hash function (Shrader Col. 8, lines 31-35 & lines 62-67 & Col. 9, lines1-2 & Col. 11, lines 47-48; teaches on the use of a single or multiple hash functions and or algorithms).

Claim 9:

The system as recited in claim 7, further comprising a validation module (Col. 2, lines 19-29 & Col. 13, lines 57-67; meets the limitation of the validation) coupled to the protected message envelope reader (Col. 12, lines 4-7 & Col. 15, lines 38-63; meets the limitations of protected message enveloped reader) and the message unmasker (Col. 12, lines 4-7& 34-46 & Col. 15, lines 38-63; reads on the unmasking/decrypting of the masked/encrypted message), the validation module comprising: a message validation code generator configured to generate a second message validation code based on the predetermined key, the unmasked message(Col. 2, lines 19-29 & Col. 13, lines 57-67; meets the limitation of the validation/authentication of the message and the key), and the random value(Shrader Col. 11, lines 47-48; teaches this because the enveloped data is constructed and generated at random); and a message validation code comparator coupled to the protected message envelope reader and the message validation code generator and configured to generate a validation based on the first message validation code and the second message validation code(Col. 2, lines 19-29 & Col. 13, lines 57-67; meets the limitation of the validation/authentication).

Claims 10-11:

Wherein the validation module employs a first one-way hash function and wherein the validation module employs a first one-way hash function and the one-time pad generator employs a second one-way hash function (Shrader Col.

8, lines 31-35 & lines 62-67 & Col. 9, lines1-2 & Col. 11, lines 47-48; teaches on the use of a single or multiple hash functions and or algorithms).

Claim 12:

A method in a message source for secure communication, comprising: generating a random value (Shrader Col. 11, lines 47-48; teaches this because the enveloped data is constructed and generated at random); generating a message validation code based on a message, the random value, a predetermined key (Col. 2, lines 19-29 & Col. 13, lines 57-67; meets the limitation of the validation/authentication and the key), and a first one-way hash function; generating a one-time pad based on the random value (Shrader Col. 11, lines 65-67; meets the limitation of generating a masked message based on the one-time pad by stating that the encrypted content/data could be padded), the predetermined key, and a second one-way hash function; generating a masked message based on the message and the one-time pad; (Shrader Col. 8, lines 31-35 & lines 62-67 & Col. 9, lines1-2 & Col. 11, lines 47-48; teaches on the use of a single or multiple hash functions and or algorithms); and transmitting a secure message that comprises the random value, the masked message, and the message validation code to a message target, wherein the message target is configured to unmask the masked message to form the message and validate the message using the message validation code (Col. 13 lines 57-67).

Claim 13:

The method as recited in claim 12, further comprising generating a protected message envelope based on the random value, the masked message, and the message validation code (Col. 11, lines 46-67; reads on the limitations of the protected message envelope, the random value along with the masked/encrypted message; Col. 2, lines 19-29 & Col. 13, lines 57-67 meet the limitations of the validation).

Claim 14:

The method as recited in claim 13, wherein the secure message comprises the protected message envelope (abstract).

Claim 15:

Wherein the first one-way hash function and the second one-way hash function are the same one-way hash function (Shrader Col. 8, lines 31-35 & lines 62-67 & Col. 9, lines1-2 & Col. 11, lines 47-48; teaches on the use of a single or multiple hash functions and or algorithms).

Claims 16-17:

(Candeled)

Claim 18:

A method in a message target for secure communication, comprising:

receiving a secure message transmitted from a message source, wherein the secure message comprises a random value, a masked message, and a first message validation code (Col. 11, lines 46-67; reads on the limitations of the protected message envelope, the random value along with the

masked/encrypted message; Col. 2, lines 19-29 & Col. 13, lines 57-67 meet the limitations of the validation); generating a one-time pad based on the random value, a predetermined key, and a first one-way hash function; and generating an unmasked message based on the one-time pad and the masked message (Shrader Col. 11, lines 65-67; meets the limitation of generating a masked message based on the one-time pad by stating that the encrypted content/data could be padded; Shrader Figure 3 & 4C & 7 & Col. 1, line 27-43 & Col. 12 lines 4-7; reads on the predetermined key limitation and the unmasking/decrypting of the masked/encrypted message).

Claim 19:

The method as recited in claim 18, further comprising: generating a second message validation code based on the unmasked message, the random value (Col. 11, lines 46-48; reads on the limitations of the random values), the predetermined key and a second one-way hash function; and comparing the first message validation code to the second message validation code to determine a validity of the unmasked message (Figures 3 & 4A-B & Col. 2 lines 19-40 & Col. 13 lines 57-67; reads on the limitations of the message validation including the decryption, the key and the hash function).

Claim 20:

The method as recited in claim 19, wherein the first one-way hash function and the second one-way hash function are the same one-way hash function

(Shrader Col. 8, lines 31-35 & lines 62-67 & Col. 9, lines1-2 & Col. 11, lines 47-48; teaches on the use of a single or multiple hash functions and or algorithms).

Claim 21:

The method of claim 18, wherein the secure message comprises a protected message envelope, the method further comprising: extracting the random value, the masked message, and the first message validation code from the received protected message envelope (Figure 5A-B & Col. 2 lines 19-32; reads on the limitations the protected message envelope; and reads on the limitations of the message validation).

Claim 22:

A computer program product for secure communications in a message source, the computer program product having a computer readable medium with a computer program embedded thereon (Col. 20 lines 12-23; reads on the medium), the computer program comprising: computer code for generating a random value (Col. 11, lines 46-48; reads on the limitations of the random value); computer code for generating a message validation code based on a message to be sent, the random value, a predetermined key, and a first one-way hash function (Col. 2, lines 19-32 & Col. 11, lines 46-61; reads on the limitations of the random value, the key, and the hash function); computer code for generating a one-time pad based on the random value, the predetermined key, and a second one-way hash function (Col. 11, lines 46-67; reads on the limitations of the padded data, the random value, the key and the hash function); computer code

for generating a masked message based on the message to be sent and the one-time pad; computer code for generating a protected message envelope based on the random value, the masked message, and the message validation code (Col. 11, lines 46-67 & Col. 13, lines 57-67; has the limitations of the masked message, the padded data, the protected message envelope, the random value and the message validation); and computer code for transmitting the protected message envelope to a message target, wherein the message target is configured to unmask the masked message to form the message and validate the message using the message validation code (Col. 13 lines 57-67 and 20 lines 3-11).

Claim 23:

A computer program product for secure communications in a message target, the computer program product having a computer readable medium with a computer program embedded thereon (Col. 20 lines 12-23; reads on the medium), the computer program comprising: computer code for receiving a protected message envelope transmitted from message source; computer code for extracting a random value (Col. 11, lines 46-48; reads on the limitations of the random value), a masked message, and a first message validation code based on the protected message envelope, wherein the random value, the message, and the first message validation code are generated at the message source (Figure 5A-B & Col. 2 lines 19-32; reads on the limitations of receiving the protected message envelope; and by stating that the system allows for recursion,

envelope nesting, and the authentication of the content of the message, reads on the limitations of the message validation); computer code for generating a one-time pad based on the random value, a predetermined key, and a first one-way hash function (Col. 11, lines 46-67 reads on the padded data, the random value, the key and the hash function); computer code for generating an unmasked message based on the one-time pad and the masked message (Col. 11, lines 65-67 & Col. 12, lines 4-7; reads on the limitation of the padded data and the decrypting/unmasking of the message); computer code for generating a second message validation code based on the unmasked message, the random value, the predetermined key, and a second one-way hash function (Col. 2, lines 19-32 & Col. 11 lines 47-48; read on the validation irrespective of number of iterations, also reads on the random factor, the key, and the hash functions); and computer code for comparing the first message validation code to the second message validation code to determine a validity of the unmasked message (Col. 2, lines 19-32; once again read on the validation irrelevant of the number of times the data is authenticated).

Examiner Note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses, to fully consider the references in its entirety as potentially teaching of all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner

Response to Arguments

5. Applicant's arguments filed have been fully considered but are not persuasive. In substance, the applicant argues A) claims 22 and 23, as currently amended, fall under a statutory category; B) none of the cited portions teach a message validation code based on a predetermined key, a message and a random value; C) Shrader does not teach the claimed features arranged as they are in claim 5.

6. In response to A), although examiner agrees with applicant where "software must be executed on some device or structurally tied to some computer readable medium to realize its function", the claims fail to explicitly meet either of these conditions. Nowhere in the claims 22 and 23 is it stated that the computer code is "executed". Furthermore the claims are not structurally tied a tangible computer readable media. The only reference in the specification appears to be directed to other non-statutory subject matter (i.e. signal, energy).

In response to B), examiner respectfully disagrees. Shrader discloses a validation code based upon a predetermined key, a message and a random value. The validation code is in part a "digital signature" (Col. 13 lines 57-67). A digital signature is a security mechanism that relies on two keys that are used to encrypt messages before transmission and to decrypt them on receipt. They are also useful in establishing non-repudiation. A digital signature is always generated by using a message and a predetermined key (Col. 11 lines 47-48). The predetermined keys of Shrader are based upon random values. Therefore, the validation code of Shrader is based on a predetermined key, a message and a random value. Therefore Shrader still meets the scope of the limitations as currently claimed.

In response to C), examiner respectfully disagrees. The applicant has simply stated structural elements with an intended use. A recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim. Regarding the order with which structural elements are presented, the order of structural elements void of any interaction therewith are not given weight. A mere structural equivalence in the prior art is sufficient to meet the scope of the limitations. A specific order of interaction must be explicitly presented in the claims. Claimed subject matter not the specification is the measure of the invention. Disclosure contained in the specification cannot be read into the claims for the purpose of avoiding prior art. In re Sporck, 55 CCPA 743, 386 F .2d 924, 155 USPQ 687 (1986); In re Self, 213 USPQ 1, 5 (CCPA 1982); In re Priest, 199 USPQ 11, 15 (CCPA 1978).

Conclusion

1. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Maceeh Anwari whose telephone number is 571-272-7591. The examiner can normally be reached on Monday-Friday 7:30-5:00 PM ES.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Vaughn can be reached on 571-272-3922. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

M.A.

WILLIAM VAUGHN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100